NATIONAL
CYBERSECURITY
CENTER

NCC King County Audit Summary 2020

NCC NATIONAL CYBERSECURITY CENTER

King County Audit Summary

March 3, 2020

Election Overview: King Conservation District Board of Supervisor Election | February 11, 2020

Total Registered Voters	Ballots Returned 2020 Election	Ballots Returned 2019	Voter Turnout Increase
1,265,576	6,280	3,241	93.77%

Technology: OmniBallot Secure Ballot Transmission System (Democracy Live)

Total ballots submitted	Total ballots returned electronically	Return rate for electronic ballots submitted	Signature approval rate
6,280	5,921	94.2%	99.63%

Election Results & Auditor Review

The National Cybersecurity Center (NCC) conducted an independent, third-party review of Democracy Live's security measures as well as the security in place at the King County Elections Office to assess the overall integrity level of the King County Conservation District election. Democracy Live's security measures are in place to prevent, detect, and mitigate any possible interference with ballot security.

The NCC reviewed Democracy Live's logs to determine there was no interference with the ballots kept in the secure Amazon Web Services (AWS) cloud. The NCC also met with King County Election Officials and IT personnel to review security procedures.

The process between King County and Democracy Live was seamless: ballots submitted online were stored in the AWS cloud and kept secure using AWS Object Lock that encrypts the ballots leaving them unable to be manipulated. After voting was completed, King County election officials downloaded and printed the ballots stored in the cloud, ran signature verification and then tabulated them according to the same standards as mail ballots.

The following audit standards were used to review the various security measures taken by the vendor and the county.

Audit standards implemented

- **Digital forensics audit** – audit of any access to the root level of the Amazon Web Services (AWS) account; review of external attempts to interrupt service[1]

Democracy Live has developed and implemented external and internal security standards that ensure that internal and external threats may be detected, recorded, prevented, and mitigated. Below are the various processes and measures utilized to protect ballot integrity:

- Democracy Live conducted regular audits of the cloud trail and documented any access times along with the reasons for the access; the National Cybersecurity Center reviewed the report for any issues. The could trail was accessed twice – once to delete test ballots generated by King County election officials prior to the election; the second time was to allow for premium support in AWS.
- Democracy Live has a process in place to confirm that no employee can download ballots stored in the cloud; the National Cybersecurity Center reviewed the process and audit log to confirm that no employees downloaded ballots.
- Democracy Live monitors all external attempts to interfere with the application programming interface (API) to create down time (a denial of service attack); Democracy Live received only one attempt. No access was gained, and no downtime was recorded. Another common attack is the injection of malicious SQL commands that can compromise the database; the site received 123 SQL injection threats during the voting period which lasted between January 22

and February 11. Democracy Live was able to able to identify and block each attempt, and no part of the system was compromised.

- **Ballot Audit** – Ensuring the number of ballots submitted via the OmniBallot Portal was received and processed by King County
    - The National Cybersecurity Center, along with King County Election Officials, confirmed that the total number of ballots returned via the application equaled the total number of ballots downloaded and tabulated. This ballot audit is important to ensure the number of ballots submitted via OmniBallot matches the number of ballot packets downloaded, printed and processed. This independent audit shows that all ballots submitted were downloaded and processed according to current paper ballot absentee processes.

- **Signature Verification** – Comparing the OmniBallot signature approval/rejection rate to the traditional, paper-marked signatures King County receives.
    - The signature approval rate of the ballots submitted online was 99.63 percent – 23 ballots were rejected for signature mismatches. The challenge rate for online ballots was 1.25 percent, less than the signature challenge rate for mail ballots returned (1.5 percent). The source of the change is likely tied to the option that voters may sign their name via their smart device touch screen. King County speculated that this higher than expected accuracy may be due to how the original signatures tend come from a digital pad which is like a smart device screen. Additionally, voters submitting mail ballots may forgot that they are required to sign the signature affidavit. The signature verification approval rate on the OmniBallot system is statistically significant and may offer increased confidence in the accuracy of signature process.

- **Ballot Tabulation** – Confirming all ballots received from OmniBallot were directly printed and tabulated into the King County tabulation scanning system.
    - The National Cybersecurity Center reviewed the tabulation process at King County Elections (KCE) with the election staff to confirm that the process was in place to ensure all ballots stored in the AWS cloud were directly downloaded by KCE, printed and processed using the same procedures as all other ballots received by KCE.

Lessons Learned & Next Steps

In review of their processes and procedures, King County Elections and Democracy Live have demonstrated proven, effective security measures to ensure that ballots have not been compromised or tampered with. Through AWS, the portal security systems are constantly monitored for any unintended or nefarious interference. The processes and transparency of both the solution and procedural systems at KCE supports the conclusion that the pilot was successfully conducted without malicious or unintended interference, and with the accuracy expected in the conduct of elections

As Democracy Live continues to support mobile voting pilots across the country, the National Cybersecurity Center looks forward to working with the company to develop a ballot auditing method akin to a risk limiting audit. By incorporating such a method, Democracy Live will effectively couple their already high security standards with a ballot audit that instills the highest levels of confidence that ballots are not impacted.

Link to election results: https://www.kingcounty.gov/depts/elections/results/ballot-return-statistics.aspx

Democracy Live makes the raw audit logs and reports of elections available upon request and approval.

About – Partners

National Cybersecurity Center – The National Cybersecurity Center exists to help secure the world using knowledge, connections and resources to solve global cybersecurity challenges and develop a protected cyber ecosystem. An independent and non-profit think tank based in Colorado Springs, Colorado, the NCC provides cybersecurity leadership, services, training and a cybersecurity community for public officials, business executives and the workforce. Discover the NCC at www.cyber-center.org.

Tusk Philanthropies – Tusk Philanthropies was created by Bradley Tusk, Founder and CEO of Tusk Holdings & Tusk Ventures, for the purpose of working on reducing hunger throughout the United States by providing greater access to programs like school breakfast and to dramatically increase voter turnout and participation in U.S.

elections through mobile voting, beginning with qualified military service members. Mobile voting is a non-partisan initiative designed to not favor any one candidate or party but to expand voting options to increase participation in our electoral process. None of the Tusk entities has a financial interest in Democracy Live or any other voting technology company.

About Democracy Live: Founded in 2007, Democracy Live provides voting and voting information technologies to the 200 million eligible voters in the U.S. In partnership with Amazon and Microsoft, Democracy Live is the largest provider of cloud and tablet-based voting technologies in the U.S.

Selected and funded by the Department of Defense and a founding participant in the Department of Homeland Security sponsored Sector Committee for Critical Voting Infrastructure, Democracy Live is a leading authority on secure voting technologies. Approved and funded in part by the Department of Health and Human Services and the Elections Assistance Commission to assist voters with disabilities, OmniBallot is the most deployed accessible online balloting platform in the U.S.

[1] More details on the various measure may be found in Democracy Live's Post Election Security Audit, February 17, 2020. The link is at the end of this report.